DIGEST

The digest printed below was prepared by House Legislative Services. It constitutes no part of the legislative instrument. The keyword, one-liner, abstract, and digest do not constitute part of the law or proof or indicia of legislative intent. [R.S. 1:13(B) and 24:177(E)]

HB 1140 Original 2026 Regular Session Mike Johnson

Abstract: Provides relative to the regulation of telecommunications.

Proposed law defines "call authentication technology" and "telecommunications provider".

Proposed law requires a telecommunications provider operating in this state to do all of the following:

(1) Implement call authentication technology consistent with federal law and regulations.

(2) Maintain and file a robocall mitigation plan consistent with federal requirements.

(3) Take reasonable steps to prevent, detect, and mitigate unlawful caller ID spoofing traffic originating on or passing through its network.

(4) Investigate credible notice from the attorney general that unlawful spoofed traffic is being transmitted over its network.

Proposed law prohibits a telecommunications provider from doing any of the following:

(1) Knowingly transmit spoofed caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value.

(2) Knowingly provide substantial assistance or support to a person engaged in unlawful caller ID spoofing.

(3) Continue to carry traffic for a customer or upstream provider after receiving written notice from the attorney general that the traffic is unlawful, unless corrective action is taken within 30 days.

Proposed law allows the attorney general to bring a civil action to enforce the provisions of proposed law for injunctive relief, civil penalties, restitution, and investigative costs.

Proposed law provides that the civil penalties shall not exceed $10,000 for a knowing violation and not exceed $1,000 for a negligent failure to implement required mitigation measures.

Proposed law provides that a telecommunications provider shall not be liable, if it meets all of the

following requirements:

(1) Implements and maintains call authentication technology and mitigation programs consistent with federal requirements.

(2) Acts in good faith to block or mitigate unlawful traffic.

(3) Does not knowingly facilitate unlawful spoofing.

Proposed law provides nothing in proposed law shall impose strict liability on a telecommunications provider solely because unlawful spoofed traffic transits its network.

Proposed law requires proposed law to be interpreted consistently with federal law and shall not be construed to conflict with federal preemption.

Proposed law provides that proposed law shall be known and may be cited as the "Stop The Calls" Act.

(Adds R.S. 51:1741.6)